REMARKS/ARGUMENTS

Applicants amended claim 16 to clarify that certain limitation were "means" limitations.

Applicants amended claim 30 to correct a typographical error.

1. The Claims Comply with the Written Description Requirement

The Examiner rejected claims 1-40 for failing to comply with the written description requirement of 35 U.S.C. §112, par. 1 on the grounds that the added requirement to claims 1, 9, 11, 16, 22, 24, 27, 35, and 37 that keys are maintained for "authorized users" is not disclosed in the application. (Final Office Action, pg. 6) Applicants amended these claims to change "users" to "computer systems". In the Final Office Action, the Examiner recognized that maintaining keys for computer systems to access the software is disclosed in the Application. During a phone conversation, the Examiner indicated he would enter this amendment to overcome the written description rejection.

Applicants submit that the claims as amended comply with the written description requirement.

2. Claims 1-4, 7-30, and 33-40 are Patentable Over the Cited Art

The Examiner maintained his rejection of claims 1-4, 7-30, and 33-40 as obvious (35 U.S.C. §103) over Ananda (U.S. Patent No. 5,495,411) in view of Takahashi (U.S. Patent No. 6,195,432). Applicants traverse for the following reasons.

Amended independent claims 1, 16, and 27 concern distributing computer software from a first computer system, and require: maintaining keys of computer systems authorized to access software to be distributed; receiving a request for software from a second computer system; generating a message; encrypting the generated message; transmitting the encrypted message to the second computer system; receiving an encrypted response from the second computer system; determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response; decrypting the encrypted response with the determined key if there is one determined key; processing the decrypted response to determine whether the second computer system is authorized to access the software, wherein the second computer system is not authorized to access the software if there is not one maintained key for

the second computer system that is capable of decrypting the encrypted response; and permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

As discussed above, Applicants amended claims 1, 16, and 27 to change "users" to "computer systems" to overcome the written description rejection.

In the Response to Arguments, the Examiner found that col. 10, line 55 to col. 11, line 58 of Takahashi teaches the claim requirement of maintaining keys of authorized systems. (Final Office action, pgs. 2-3) The claims require that the keys of the authorized systems are used to decrypt responses from an authorized customer system (second computer system) to check whether the response permits access, where access to the software is not permitted if there is not one key maintained for the second system. The cited cols. 10-11 of Takahashi mention that a user information store has an ID and shared key for the customer. Takahashi mentions the customer side sends the encrypted shared key to the store side. (Takahashi, col. 9, lines 18-25) The store side stores in the information storage unit the ID, shared key, and credit card information assigned to customers. (Takahashi, col. 10, lines 64-68)

Nowhere does the cited Takahashi teach or suggest the claim requirements that the cited shared key is used by the first computer system (distributor of the software) to decrypt a response from the second computer system (customer system), where the requesting customer is not authorized to access the software if there is not one maintained key capable of decrypting the response. Instead, according to Takahashi, the customer side uses the shared key 202 to generate a hash value 205 that is sent to the server with the product specifying data. The server side then has its own copy of the shared key 103 to obtain a server hash value 205', and if the customer sent hash value 205 and server hash value 205' coincide, the order is proper and the software may be transmitted. (Takahashi, col. 11, line 61 to col. 12, line 52). Thus, according to Takahashi the cited hash value is not sent to the server side and used by the server to decrypt an encrypted response that is part of a request for software. Instead, the cited shared value is used to generate a hash value that the customer transmits with the product specifying data. (Takahashi, col. 12, lines 17-25). Nowhere does the cited Takahashi teach or suggest that the shared value is used to decrypt a response from the customer side.

In the Response to Arguments, the Examiner further cited col. 12, line 20 to col 13, line 33 as teaching the requirement of determining whether there is a key to decrypt a response, wherein the customer (second) computer is not authorized to access the software if there is not a key for the user. (Final Office Action, pg. 3, par. 4) As discussed, this cited section of Takahashi concerns the distributor side (first computer) determining whether there is a hash key for the customer ID that can produce a server hash value 205' coinciding with the customer hash value 205. As discussed, the cited shared key or has value generated therefrom are not used to decrypt messages as claimed.

Moreover, the claims require processing the decrypted response to determine whether the customer (first computer) is permitted to access the software. Nowhere does the cited Takahashi teach processing a decrypted response to a message to determine whether access is permitted. Instead, the cited Takahashi compares a customer hash value 205 sent with a message with a server hash value 205' to determine whether access is permitted.

Thus, the cited of Takahashi does not teach or suggest keys used by the distributor side (first computer system) to decrypt responses from the customer side (second computer system) as claimed. Instead, the cited "shared key" of Takahashi is not used for decrypting responses as claimed and is instead used to generate a hash value sent with product specifying data.

Moreover, the sections of Ananda the Examiner cited in the Response to Arguments also fails to teach or suggest the above discussed claim requirements concerning maintaining keys for authorized computer systems used to decrypt a received response and determine whether the requesting customer (second computer system) is authorized to access the software. The Examiner cited col. 11, lines 45-60 and col. 12, lines 15-46 of Ananda as teaching various claim limitations. (Final Office Action, pgs. 4-5, 7-8) A review of the cited Ananda reveals that Ananda is concerned with components in the user computer that process a message to determine whether access is authorized, not the central server. The cited col. 11 of Ananda mentions that the password generation module 321E generates a new authorization verification password that is stored as a function of the processor clock time. However, the cited password generation module 321E is part of the user computer 102 (FIG. 2) because it is part of the header software 284A shown in FIG. 3, not part of the software distributing system. The user is the requestor of software, not the distributor. Ananda mentions that as shown in FIG. 2, the application software

284B is integrated with header software 284A, which comprises the rental application software 284. (Col. 9, lines 50 to col. 10, line 40). The rental security manager prepares and encrypts a message having information on the user (the user clock time, user ID password, and ID number of the application), which is sent to the multiuser controller 222 at the central facility that enables access to the software.

Nowhere does this cited col. 11 of Ananda anywhere disclose the claim requirements that the rental manager or other related component, which is in the user computer, maintain keys for authorized computer systems of the software, where the keys are used to decrypt encrypted responses and that the second computer (user computer) is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response. Instead, the cited col. 11 of Ananda discusses how the user computer generates a message to send to the central facility 180. Because the cited col. 11 concerns operations of the user computer to generate an authorization verification password, nowhere does the cited col. 11 teach or suggest the claim requirements of maintaining keys for authorized users of the software, where the keys are used to decrypt responses to determine whether the second computer providing the response is authorized to use the software.

The cited col. 12 of Ananda discusses how the multiuser controller 222, which is part of the database that distributes the software, generates and encrypts a new message, and sends the message to the user as part of an authorization verification process. The rental security manager 321 in the user computer receives the message. The rental security manager 321 is part of the user computer because it is part of the header software 284A shown in FIG. 3. The user computer decrypts the message and has a password validation module 321 that uses a password correlation algorithm to compare the message against stored information regarding the user processor clock time, ID, etc. When the correlation function is successful, authorization verification is complete and the header 320 in the user computer allows application software to execute.

The cited col. 12 discusses how components in the user computer compare a message from the central facility to determine whether the application can continue to execute. Nowhere does the cited col. 12 anywhere disclose the claim requirement of maintaining keys for authorized computer systems of the software, where the keys are used to decrypt encrypted responses and that the second computer is not authorized to access the software if there is not one

maintained key for the second computer system that is capable of decrypting the encrypted response. Instead, the cited col. 12 discusses how the user computer can correlate the content of a message with stored information to determine whether the application can start running. The cited col. 12 does not teach maintaining keys to use to verify whether a user requesting access is authorized as claimed. Instead, with the cited col. 12, the authorization is done at the user system, not at the central facility or distributor.

Thus, the cited Ananda and Takahashi, alone or in combination, do not teach or suggest that the distributor side (first computer system) maintains keys from authorized computer systems (customers) to decrypt responses from the customer side (second computer system) to determine whether the requesting customer system is permitted to access the software.

For all the above reasons, the amended claims 1, 16, and 27 are patentable over the cited combination, because the cited references, alone or in combination, do not teach or suggest all the claim requirements.

Claims 2-4, 8-11, 17-19, 21-24, 28-30, and 34-40 are patentable over the cited art because they depend, directly or indirectly, from one of claims 1, 16, and 27. Moreover, certain of these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

Claims 4, 19, and 30 depend from claims 1, 16, and 27, respectively, and further require that generating the message further comprises generating a random component to include within the message, and that determining whether the second computer system is authorized to access the software further comprises determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message.

In the Response to Arguments, the Examiner cited col. 11, line 9 to col. 12, line 64 of Ananda as teaching the additional requirements of these claims. (Final Office Action, pgs. 4-5) Applicants traverse. According to the cited Ananda, the multiuser controller 222 at the central facility generates an encrypted password that is sent to the rental security manager 321, which is part of the user computer, to decrypt and determine whether access is permitted. The rental

security manager 321 is part of the header software 284a within the user computer. (Ananda, col. 9, line 55 to col. 10, line 33, FIGs. 2 and 3)

Nowhere does the cited Ananda anywhere disclose that the first computer system or central facility, determine whether the user is authorized to access the software by determining whether the decrypted response includes a generated message the first computer system, or central facility, sent to the user (second computer system.) Instead, with the cited Ananda, components in the user computer determine whether access may continue. The cited Ananda does not have the central facility determine whether the user (second computer system) may access the software by checking whether the encrypted response has a generated message the first computer system (central facility) previously sent as claimed.

Accordingly, amended claims 4, 19, and 30 provide additional grounds of patentability over the cited art.

Claims 8, 21, and 34 depend from claims 1, 16, and 27, respectively, and further require that processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

The cited Ananda does not disclose that the first computer system (or central facility in Ananda) determines whether the message in the encrypted response from the second computer system matches the generated message the first computer system initially sent to the second computer system. Instead, the cited Ananda has the user computer system compare stored information with a message from the central facility, likened to the first computer system, to determine whether access is permitted. Nowhere does the cited Ananda anywhere disclose that the central facility, likened to the first computer system, compare a message in an encrypted response from the user computer, likened to the second computer system, to determine whether it matches the generated message the central facility (first computer system) previously sent to the user computer (second computer system). Thus, the cited operations of Ananda are different from the claimed operations.

Accordingly, claims 8, 21, and 34 provide additional grounds of patentability over the cited art.

Independent claims 12 and 25 concern accessing computer software from a first computer system with a second computer system and require that the second computer system perform: providing a key to the first computer system capable of decrypting an encrypted response from the from the second computer system; transmitting a request for the software to the first computer system; receiving an encrypted message from the first computer system; processing the encrypted message to generate a response message; encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided key at the first computer system; transmitting the encrypted response message to the first computer system; and receiving access to the requested software in response to the encrypted response message.

In the Response to Arguments, the Examiner cited the same sections of Ananda and Takahashi against claims 12 and 25 that were cited against independent claims 1, 16, and 27. (Final Office Action, pgs. 4-5, par. 6)

The cited Ananda discusses how a user computer generates an authorization verification password and sends an encrypted message with various information to the central facility. A multi-user controller 22 at the central facility generates a message to send back to the user computer. The user computer header software then verifies the received message from the central facility with the stored authorization verification password.

Nowhere does the cited Ananda anywhere teach or suggest the claim requirement of the second computer (user computer) providing a key to the first computer, and then transmitting a response to the first computer that can be decrypted by the sent key at the distributor computer (first computer), and then receiving access to the requested software in response to the encrypted response message.

The cited Takahashi discusses the shared key. As discussed above, the shared key of Takahashi is used to generate a hash code that the user computer sends to the distributor. Nowhere does the cited Takahashi teach or suggest that this shared key provided to the distributor computer is used to encrypt a response message that is capable of being decrypted by the provided key at the distributor (first computer system).

Accordingly, claims 12 and 25 are patentable over the cited Ananda and Takahashi because the cited art does not disclose all the claim requirements.

Claims 13-15 and 26 are patentable over the cited art because they depend from claims 12 and 25, respectively, which are patentable over the cited art for the reasons discussed above.

Claims 38-40 are patentable over the cited art because they depend, directly or indirectly, from claim 26, which is patentable over the cited art for the reasons discussed above.

3. Claims 5, 6, 31, and 32 are Patentable Over the Cited Art

The Examiner rejected claims 5, 6, 31, and 32 as obvious (33 U.S.C. 103) over Ananda in view of Komura (U.S. Patent No. 5,994,307). (Final Office Action, pgs. 9-10) Applicants traverse this rejection on the grounds that these claims depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Moreover, these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

First off, claims 5, 6, 31, and 32 are patentable over the cited art because they depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Further, these claims provide additional grounds of distinction over the cited art for the following reasons.

Claims 5 and 31 depend from claims 1 and 27, respectively, and further require that the random component is comprised of a time stamp. The Examiner cited Komura as teaching the time stamp claim requirement. (Final Office Action, pgs. 9-10) Applicants traverse.

Although the cited Komura does discuss a timestamp and Ananda mentions that a clock time is used to calculate a pseudo number password, nowhere does the cited Ananda, Takahashi or Komura, alone or in combination, anywhere teach or suggest that a message generated and encrypted and sent to a second computer system, which is then included in an encrypted response by the second computer system to the first computer system, comprises a timestamp.

Accordingly, claims 5 and 31 provide additional grounds of patentability over the cited art.

Claims 6 and 32 depend from claims 5 and 31 and further require that the time stamp is inserted at an offset into the message. These claims are patentable over the cited combination because they depend from claims 5 and 31, which are patentable over the cited art for the reasons discussed above, and because they provide further requirements on the timestamp, which is not disclosed in the cited Ananda.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-40 are patentable over the art of record. Applicants submit that no additional fees are needed. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: April 25, 2005

By: _____
David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984